REMARKS

The Office Action dated August 16, 2008 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. Claims 1-56 are currently pending in the application and are respectfully submitted for consideration.

Claims 1, 2, 4, 5, 27, 34, 35, 43, 49, 51, and 55-56 were rejected under 35 U.S.C. §102(e) as being anticipated by Bolosky et al. (U.S. Patent No. 7,043,637). This rejection is respectfully traversed for at least the following reasons.

Claim 1, upon which claims 2-33, depend is directed to a method including generating a second set of data representative of a first set of data. The method also includes encrypting the first set of data using the second set of data.

Claim 34, upon which claims 35-54, depend is directed to a system including a generating unit configured to generate a second set of data representative of a first set of data. The system also includes an encrypting unit configured to encrypt the first set of data using the second set of data.

Claim 55, upon which claim 56 is dependent, recites a system including generating means for generating a second set of data representative of a first set of data, and encrypting means for encrypting the first set of data using the second set of data.

Embodiments of the present invention therefore provide easy and secure access to archived digital images and further provide efficient and cost effective ciphering. The efficiency and simplicity of the present invention may also optimise resource

consumption in end user devices and in archives. An additional advantage of the present invention is that there may be no need for administrators to have access to the secured information. Additionally, a further advantage of embodiments of the present invention is that using an image which is representative of the original image as a ciphering key may provide an extremely useful description of the content of the original image.

As will be discussed below, the cited prior art fails to disclose or suggest all of the elements of the claims, and therefore fails to provide the advantages and features discussed above.

Bolosky discloses a file format for a serverless distributed file system, which is composed of two parts: a primary data stream and a metadata stream. The data stream contains a file that is divided into multiple blocks. Each block is encrypted using a hash of the block as the encryption key. The metadata stream contains a header, a structure for indexing the encrypted blocks in the primary data stream, and some user information. The indexing structure defines leaf nodes for each of the blocks. Each leaf node consists of an access value used for decryption of the associated block and a verification value used to verify the encrypted block independently of other blocks. In one implementation, the access value is formed by hashing the file block and encrypting the resultant hash value using a randomly generated key. The key is then encrypted using the user's key as the encryption key. The verification value is formed by hashing the associated encrypted block using a one-way hash function. The file format supports verification of individual file blocks without knowledge of the randomly generated key or any user keys. To verify

Application No.: 10/619,176

a block of the file, the file system traverses the tree to the appropriate leaf node associated with a target block to be verified. The file system hashes the target block and if the hash matches the access value contained in the leaf node, the block is authentic.

Applicants respectfully submit that Bolosky fails to disclose or suggest all of the elements of the present claims. For example, Bolosky does not disclose or suggest "generating a second set of data representative of the first set of data," as recited in claim 1 and similarly recited in claims 34 and 55.

As discussed above, Bolosky teaches a file format for a serverless distributed file system that includes a primary data stream and a metadata stream. The data stream contains a file that is divided into multiple blocks that are each hashed with a hash function to produce a hash value. Each hash value is then used to encrypt the block to which it corresponds. The Office Action alleged that the Bolosky hash values are "representative" of the Bolosky file (Office Action, page 3). However, a close reading of Bolosky demonstrates that the hash values are simply not disclosed as being representative of the file, unlike the second set of data that is representative of the first set of data, as recited in claim 1. Indeed, the Bolosky hash values appear to share no direct, inherent relationship with one another at all. Furthermore, Bolosky does not appear to disclose or suggest any motivation, benefit, or interest in producing hash values that collectively represent the file, likely because doing so would simply not facilitate achieving any of the objectives of the Bolosky invention.

Application No.: 10/619,176

Accordingly, Bolosky fails to disclose or suggest "generating a second set of data representative of the first set of data," as recited in claim 1 and similarly recited in claims 34 and 55. As such, Applicants respectfully request that the rejection of claims 1, 34, and 55 be withdrawn.

Claims 2, 4, 5, 27, 35, 43, 49, 51, and 56 are dependent upon claims 1, 34, and 55, respectively. Therefore, claims 2, 4, 5, 27, 35, 43, 49, 51, and 56 should be allowed for at least their dependence upon claims 1, 34, and 55, and for the specific limitations recited therein.

Claims 1, 2, 4, 5, 27, 34, 35, 43, 49, 51, and 55-56 were also rejected, alternatively, under 35 U.S.C. §103(a) as being unpatentable over Bolosky. This rejection is respectfully traversed for at least the following reasons.

As outlined above, Bolosky fails to disclose or suggest "generating a second set of data representative of the first set of data," as recited in claim 1 and similarly recited in claims 34 and 55. Furthermore, Applicants respectfully assert that a person of ordinary skill in the art would not have been motivated to modify Bolosky to yield the claimed invention. In fact, the Office Action did not provide any statement or reasoning for why a person of skill in the art would be motivated to modify Bolosky. Accordingly, the Office Action has failed to provide a prima facie case for obviousness. Applicants, therefore, respectfully request that the rejection of claims 1, 2, 4, 5, 27, 34, 35, 43, 49, 51, and 55-56 under §103(a) be withdrawn.

Application No.: 10/619,176

Claims 3 and 36 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Schneier ("Applied Cryptography", 1996, Second Edition, John Wiley and Sons, Inc., pages 13-14). The Office Action took the position that Bolosky discloses all of the elements of the claims, with the exception of the first set of data being encrypted by performing an exclusive OR operation between the first set of data and the second set of data. The Office Action then cited Schneier as allegedly curing this deficiency in Bolosky. This rejection is respectfully traversed for at least the following reasons.

Bolosky is discussed above. Schneier discloses a simple XOR algorithm. Schneier further teaches that the XOR algorithm is a symmetric algorithm where plaintext is XORed with a keyword to generate the ciphertext. Encryption using an XOR algorithm is also disparaged as being insecure and trivial to break.

Claims 3 and 36 are dependent upon claims 1 and 34, respectively. As presented above, Bolosky does not disclose or suggest "generating a second set of data representative of the first set of data" as recited in claim 1 and similarly recited in claim 34. Additionally, Schneier does not cure this deficiency in Bolosky. Rather, Schneier only contains a brief explanation and example of a simple-XOR algorithm. Furthermore, Applicants submit that there is no motivation to combine Bolosky and Schneier, either found in the references themselves or in the knowledge available to a person of ordinary skill in the art at the time the invention was made. Accordingly, Applicants submit that

Application No.: 10/619,176

claims 3 and 36 recite subject matter which is neither disclosed nor suggested by the combination of Bolosky and Schneier.

Claims 6, 7, 9-11, 16, 18, 19, 21-24, 26, 29, 30, 37, 38, 40, and 46 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Suzuki et al. (U.S. Patent No. 6,704,119). This rejection is respectfully traversed for at least the following reasons.

Bolosky is discussed above. Suzuki discloses a file system in which a processing apparatus is coupled to a storage unit. The processing apparatus includes a copy function for reading image data and printing the read image data on a sheet, a transmitting function for transmitting image data and/or character data via a communication line, and/or a printing function for printing received image data and/or character data on a sheet. The file system includes storage management means for automatically causing the storage unit to store data equal to processed data corresponding to a processing result obtained by the function provided in the processing apparatus, and output management means for outputting the data read from the storage unit in response to a processing instruction supplied to the file system. The storage management means has information obtaining means for obtaining specifying information specifying data to be stored by the storage unit so that the data to which the specifying information is added is stored by the storage unit. The output management means has display means for displaying either at least a part of each of data items stored by the storage unit or specifying information items specifying the data items, and operation means for selecting an item from among

Application No.: 10/619,176

the items displayed by the display means and inputting the processing instruction, so that a data item corresponding to the selected item is output in response to the input processing instruction.

Claims 6, 7, 9-11, 16, 18, 19, 21-24, 26, 29, 30, 37, 38, 40, and 46 are dependent upon claims 1 and 34, respectively. As discussed above, Bolosky does not disclose or suggest "generating a second set of data representative of the first set of data" as recited in claim 1 and similarly recited in claim 34. Additionally, Suzuki does not cure this deficiency in Bolosky. Rather, Susuki discloses a file system which includes a storage management system for automatically causing the storage unit to store data equal to processed data. Hence, the combination of Bolosky and Suzuki fails to disclose or suggest all of the elements of claims 6, 7, 9-11, 16, 18, 19, 21-24, 26, 29, 30, 37, 38, 40, and 46. Furthermore, Applicants submit that there is no motivation to combine Bolosky and Schneier, either found in the references themselves or in the knowledge available to a person of ordinary skill in the art at the time the invention was made. Accordingly, Applicants submit that claims 3 and 36 recite subject matter which is neither disclosed nor suggested by the combination of Bolosky and Schneier.

Claims 8, 12-15, 20, 25, 39, and 52 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Suzuki, and further in view of Marvit et al. (U.S. Patent No. 6,625,734). This rejection is respectfully traversed for at least the following reasons.

Application No.: 10/619,176

Bolosky and Suzuki are discussed above. Marvit discloses a method for controlling and tracking access to a message that is communicated from a first node to a second node in a network. According to the method, a request is received from the first node for a message identifier that uniquely identifies the message and a key that may be used to encode the message. Both the message identifier and the key are generated in response to the request. Both the message identifier and the key are provided to the first node to allow the message to be encoded with the key to generate an encoded message. A request is received from the second node for the key. The key is provided to the second node to allow the encoded message to be decoded and the message to be retrieved using the key. Finally, the key is deleted based upon specified key policy criteria to prevent copies of the encoded message from being decoded.

Claims 8, 12-15, 20, 25, 39, and 52 are dependent upon claims 1 and 34, respectively. As outlined above, the combination of Bolosky and Suzuki fails to disclose or suggest all of the elements of claims 1 and 34. Marvit does not cure this deficiency in Bolosky and Suzuki, as Marvit also fails to disclose or suggest "generating a second set of data representative of the first set of data." Therefore, the combination of Bolosky, Suzuki and Marvit fails to disclose or suggest all of the elements of claims 8, 12-15, 20, 25, 39, and 52.

Claim 17 was rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Suzuki, and further in view of Schneier. This rejection is respectfully traversed for at least the following reasons.

Application No.: 10/619,176

Claim 17 is dependent upon claim 1 and inherits all of the limitations thereof. As discussed above, Bolosky, Suzuki and Schneier, whether considered individually or combined, fail to disclose or suggest "generating a second set of data representative of the first set of data," as recited in claim 1. As such, the combination of Bolosky, Suzuki and Schneier fails to disclose or suggest all of the elements of claim 17.

Claims 28 and 50 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Bloomberg (U.S. Patent No. 5,765,176). This rejection is respectfully traversed for at least the following reasons.

Bolosky is discussed above. Bloomberg discloses that encoded data embedded in an iconic, or reduced size, version of an original text image is decoded and used in a variety of document image management applications to provide input to, or to control the functionality of, an application.

Claims 28 and 50 are dependent upon claims 1 and 34, respectively. As discussed above, Bolosky does not disclose or suggest "generating a second set of data representative of the first set of data," as recited in claim 1 and similarly recited in claim 34. Additionally, Bloomberg does not cure this deficiency in Bolosky since Bloomberg also does not disclose or suggest "generating a second set of data representative of the first set of data." Accordingly, the combination of Bolosky and Bloomberg does not disclose or suggest all of the elements of claims 28 and 50.

Application No.: 10/619,176

Claim 31 was rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Suzuki, and further in view of Wang et al. (U.S. Patent No. 6,173,406). This rejection is respectfully traversed for at least the following reasons.

Bolosky and Suzuki are discussed above. Wang discloses that the uniform resource locator (URL) code associated with a page provided by a world wide web server to a user is stored and provided to a media server which maintains a data base of documents and corresponding authorized URL profiles. When a user requests real-time presentation of selected media content, the user communicates the document name and URL prefix to the media server cooperating in user presentation of the selected content for authentication. If it is determined that there is no authorized correspondence with the indicated URL prefix and the document name provided, then the user node is notified that the requested presentation is unauthorized.

Claim 31 is dependent upon claim 1. As outlined above, the combination of Bolosky and Suzuki fails to disclose or suggest all of the elements of claim 1. Wang does not cure this deficiency in Bolosky and Suzuki, as Wang also fails to disclose or suggest "generating a second set of data representative of the first set of data." Therefore, the combination of Bolosky, Suzuki and Wang fails to disclose or suggest all of the elements of claim 31.

Claims 32 and 33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Suzuki, and further in view of Sull et al. (U.S. Patent

Application No.: 10/619,176

Application Publication No. 2002/0069218). This rejection is respectfully traversed for at least the following reasons.

Bolosky and Suzuki are discussed above. Sull discloses a method and system for tagging, indexing, searching, retrieving, manipulating, and editing video images on a wide area network such as the Internet. A first set of methods is provided for enabling users to add bookmarks to multimedia files, such as movies, and audio files, such as music. The multimedia bookmark facilitates the searching of portions or segments of multimedia files, particularly when used in conjunction with a search engine. Additional methods are provided that reformat a video image for use on a variety of devices that have a wide range of resolutions by selecting some material (in the case of smaller resolutions) or more material (in the case of larger resolutions) from the same multimedia file.

Claims 32 and 33 are dependent upon claim 1. As outlined above, the combination of Bolosky and Suzuki fails to disclose or suggest all of the elements of claim 1. Sull does not cure this deficiency in Bolosky and Suzuki, as Sull also fails to disclose or suggest "generating a second set of data representative of the first set of data." Therefore, the combination of Bolosky, Suzuki and Sull fails to disclose or suggest all of the elements of claims 32 and 33.

Claims 41, 42, 44, 45, and 47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Schneier, and further in view of Suzuki. This rejection is respectfully traversed for at least the following reasons.

Application No.: 10/619,176

Claims 41, 42, 44, 45, and 47 are dependent upon claim 34 and inherit all of the limitations thereof. As discussed above, Bolosky, Schneier, and Suzuki, whether viewed individually or combined fail to disclose or suggest "a generating unit configured to generate a second set of data representative of a first set of data," as recited in claim 34. Therefore, the combination of Bolosky, Schneier, and Suzuki fails to disclose or suggest all of the elements of claims 41, 42, 44, 45, and 47.

Claim 48 was rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Schneier, and further in view of Marvit (U.S. Patent No. 6,625,734). This rejection is respectfully traversed for at least the following reasons.

Claim 48 is dependent upon claim 34. As discussed above, Bolosky, Schneier, and Marvit, whether viewed individually or combined fail to disclose or suggest "a generating unit configured to generate a second set of data representative of a first set of data," as recited in claim 34. Therefore, the combination of Bolosky, Schneier, and Marvit fails to disclose or suggest all of the elements of claim 48.

Claims 53 and 54 were rejected under 35 U.S.C. §103(a) as being unpatentable over Bolosky in view of Marvit. This rejection is respectfully traversed for at least the following reasons.

Claims 53 and 54 are dependent upon claim 34 and inherit all of the limitations thereof. Additionally, as discussed above, Bolosky and Marvit, whether considered alone or in combination, fail to disclose or suggest "a generating unit configured to generate a second set of data representative of a first set of data," as recited in claim 34.

Application No.: 10/619,176

Accordingly, the combination of Bolosky and Marvit fails to disclose or suggest all of the elements of claims 53 and 54.

For at least the reasons discussed above, Applicants respectfully submit that the cited prior art fails to disclose or suggest all of the elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unanticipated and unobvious. It is therefore respectfully requested that all of claims 1-56 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

Application No.: 10/619,176

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Majid S. AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:ksh

Enclosures: Notice of Appeal
Petition for Extension of Time
Check No. 18133

Application No.: 10/619,176